P14683-A

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月　２日

出願番号
Application Number: 特願２００１－１０３０５８

出願人
Applicant(s): 日本電信電話株式会社

２００１年　６月１３日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０５５４３６

【書類名】　特許願

【整理番号】　NTTH127203

【提出日】　平成13年 4月 2日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/62

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　斎藤　賢一

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　重松　智志

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　町田　克之

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　首藤　啓樹

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　足立　卓也

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100064621

【弁理士】

【氏名又は名称】　山川　政樹

【電話番号】　03-3580-0961

【手数料の表示】

【予納台帳番号】　006194

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701512

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ゲート開閉システム

【特許請求の範囲】

【請求項１】　会場の入場ゲートを開閉するゲート開閉システムにおいて、

利用者の生体情報に基づき利用者本人を認証する認証トークンと、

利用者が前記会場の入場料の前払いを行うと前記利用者の識別情報が記憶されるデータベースと、

利用者の前記会場への入場時に前記認証トークンにより前記利用者が本人であると認証されこの認証トークンに予め記憶されている前記利用者の識別情報が前記認証トークンから出力されると、この識別情報を受信するとともに受信した識別情報が前記データベース内に記憶されている場合は前記入場ゲートを開放する制御手段と

を有することを特徴とするゲート開閉システム。

【請求項２】　会場の入場ゲートを開閉するゲート開閉システムにおいて、

利用者の識別情報が記憶される認証トークンと情報の授受を行う情報授受手段と、

利用者が前記会場の入場料の前払いを行うと前記利用者の識別情報が記憶されるデータベースと、

利用者の前記会場への入場時に前記利用者の生体情報に基づき前記認証トークンにより利用者本人であると認証されこの認証トークンから出力される利用者の識別情報が前記情報授受手段により受信されると、この受信識別情報が前記データベース内に記憶されている場合は前記入場ゲートを開放する制御手段と

を有することを特徴とするゲート開閉システム。

【請求項３】　請求項１または２において、

前記認証トークンは、利用者の指紋情報に基づき利用者本人を認証する指紋認証トークンであって、

利用者の指紋情報を記憶する記憶手段と、

利用者の指紋を検出する指紋センサと、

前記指紋センサの検出情報と前記記憶手段の記憶情報との一致に基づき前記利

用者を本人と認証する処理手段と

を有することを特徴とするゲート開閉システム。

【請求項４】　請求項３において、

前記指紋認証トークンが挿入され、かつ利用者が前記会場の入場料の前払いを行うと、パスワードを生成して生成したこのパスワードを前記指紋認証トークンに前記識別情報として記憶させるとともに、前記データベースに送信して前記利用者の識別情報として記憶させる識別情報付与手段を備えたことを特徴とするゲート開閉システム。

【請求項５】　請求項３において、

前記指紋認証トークンには予め利用者の識別番号が前記識別情報として記憶され、

前記指紋認証トークンが挿入され、かつ利用者が前記会場の入場料の前払いを行うと、前記指紋認証トークンの識別情報を読み取って前記データベースに送信し前記利用者の識別情報として記憶させる識別情報付与手段を備えたことを特徴とするゲート開閉システム。

【請求項６】　請求項１ないし５の何れかにおいて、

前記認証トークンに付加されこの認証トークンから出力される識別情報を無線信号または赤外線信号に変換して送信する送信手段と、

前記入場ゲートの近傍に配設され前記送信手段により送信される無線信号または赤外線信号を受信すると、受信した無線信号または赤外線信号に含まれる前記識別情報を前記制御手段に送出する受信手段と

を備えたことを特徴とするゲート開閉システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンサート会場や競技場の入場ゲートの開閉を行うゲート開閉システムに関する。

【０００２】

【従来の技術】

コンサート会場で催される所望のコンサートを聴く場合、利用者は予め該当するコンサートのチケットを購入し、コンサート開演前にその会場のゲート近傍の係員にそのチケットを手渡すとともに、係員がそのチケットをチェックすることにより利用者のコンサート会場への入場を許可するようにしている。

また、例えばサッカー競技場で行われるサッカーの試合を見物する場合も、利用者は同様に予めチケットを購入し、試合開始前にその競技場のゲート近傍の係員にそのチケットを手渡すとともに、係員がそのチケットをチェックすることにより利用者の競技場への入場を許可するようにしている。

【０００３】

【発明が解決しようとする課題】

しかしながら、こうしたコンサート会場や競技場への入場時に係員がチケットをチェックする方法では、チケットのチェックに多くの係員が必要になるとともに、利用者がコンサート会場や競技場への入場するのに長時間を要するという問題があった。また、利用者のチケットが盗難に遭った場合、そのチケットを利用した第三者による会場への不正入場が行われてしまうという問題もあった。

【０００４】

したがって、本発明は、利用者のコンサート会場や競技場への入場の際にチケットのチェックを行う係員を要することなくかつ利用者の速やかな入場を可能にするとともに、コンサート会場や競技場への第三者による不正な入場を阻止することを目的とする。

【０００５】

【課題を解決するための手段】

このような課題を解決するために本発明は、会場の入場ゲートを開閉するゲート開閉システムにおいて、利用者の生体情報に基づき利用者本人を認証する認証トークンと、利用者が前記会場の入場料の前払いを行うと利用者の識別情報が記憶されるデータベースと、利用者の前記会場への入場時に認証トークンにより利用者が本人であると認証されこの認証トークンに予め記憶されている利用者の識別情報が認証トークンから出力されると、この識別情報を受信するとともに受信した識別情報がデータベース内に記憶されている場合は入場ゲートを開放する制

御手段とを備えるようにしたものである。

この場合、認証トークンを、利用者の指紋情報を記憶する記憶手段と、利用者の指紋を検出する指紋センサと、指紋センサの検出情報と記憶手段の記憶情報との一致に基づき前記利用者を本人と認証する処理手段とからなる指紋認証トークンにより構成したものである。

【０００６】

また、本システムは、指紋認証トークンが挿入され、かつ利用者が前記会場の入場料の前払いを行うと、パスワードを生成して生成したこのパスワードを指紋認証トークンに識別情報として記憶するとともに、データベースに送信して利用者の識別情報として記憶させる識別情報付与手段を設けたものである。

また、本システムは、指紋認証トークンに予め利用者の識別番号を識別情報として記憶し、かつ指紋認証トークンが挿入され、利用者が前記会場の入場料の前払いを行うと、指紋認証トークンの識別情報を読み取ってデータベースに送信し利用者の識別情報として記憶させる識別情報付与手段を設けたものである。

また、本システムは、認証トークンに付加されこの認証トークンから出力される識別情報を無線信号または赤外線信号に変換して送信する送信手段と、入場ゲートの近傍に配設され送信手段により送信される無線信号または赤外線信号を受信すると、受信した無線信号または赤外線信号に含まれる識別情報を制御手段に送出する受信手段とを設けたものである。

【０００７】

【発明の実施の形態】

以下、本発明について図面を参照して説明する。

図１は、本発明に係るゲート開閉システムの構成を示すブロック図であり、本システムは、コンサート会場や競技場に設けられたゲートの開閉を行うものである。

【０００８】

図１において、本システムは、チケット販売店及び利用者の自宅に設けられ後述の指紋認証トークンが挿入され利用者がチケット代金を支払うとパスワード等を発生して指紋認証トークンに保存させるクレードル１０１と、クレードル１０

１とネットワーク１０５を介して接続されたデータベース１０２と、データベース１０２に接続されるとともに、コンサート会場や競技場に設けられたゲート１０４近傍に配置されゲート１０４の開閉を制御するゲートコントローラ１０３と、前述の指紋認証トークン１０６と、無線通信ユニット１０７と、赤外線通信ユニット１０８と、ゲート１０４の近傍に配置され無線通信ユニット１０７または赤外線通信ユニット１０８からの信号を受信してゲートコントローラ１０３に出力する無線／赤外線信号受信装置１０９とからなる。

【０００９】

前記クレードル１０１に差し込まれる指紋認証トークン１０６は、利用者が所持し、持ち運びのできる小型、軽量の装置であって、図２に示すように、本体部２０１が設けられているとともに、本体部２０１に、指紋センサ２０２と、処理装置２０３と、記憶装置２０４と、クレードル１０１との接続端子である端子２０５とが設けられている。そして、処理装置２０３は、指紋センサ２０２，記憶装置２０４及び端子２０５に接続されている。

【００１０】

また、前記無線通信ユニット１０７は、図３に示すように、指紋認証トークン１０６にアダプタ３０１を接続したものである。アダプタ３０１内には指紋認証トークン１０６の処理装置２０３と端子２０５を介して接続され処理装置２０３の出力信号を無線信号に変換する無線信号発生回路３０３が設けられ、この無線信号発生回路３０３とアンテナ３０２が接続される。

【００１１】

また、前記赤外線通信ユニット１０８は、図４に示すように、指紋認証トークン１０６にアダプタ４０１を接続したものである。アダプタ４０１内には指紋認証トークン１０６の処理装置２０３と端子２０５を介して接続され処理装置２０３の出力信号を赤外線信号に変換する赤外線信号発生回路４０３が設けられ、この赤外線信号発生回路４０３と赤外線光源４０２が接続される。

【００１２】

図１２は前記指紋認証トークン１０６を構成する指紋センサ２０２の概略的な断面を示す図である。本指紋センサ２０２は、例えばシリコンからなる半導体基

板２１１上の下層絶縁膜２１２上に形成された層間絶縁膜２１４上に、たとえば８０μｍ角の複数のセンサ電極２１５と、格子状のアース電極２１６とを備え、複数のセンサ電極２１５とアース電極２１６とを、層間絶縁膜２１４表面で規定される同一平面上に配置している。

【００１３】

センサ電極２１５は、層間絶縁膜２１４上に形成されたパシベーション膜２１７で覆い、１５０μｍ間隔に複数個を備えるようにするとともに、Ａｕから構成し、膜厚１μｍ程度に形成している。パシベーション膜２１７の膜厚は３μｍ程度としたので、センサ電極２１５上には、パシベーション膜２１７が約２（＝３－１）μｍ存在している。このパシベーション膜２１７は、例えばポリイミドなどの比誘電率が４．０程度の絶縁物から構成される。

【００１４】

上記下層絶縁膜２１２上には、センサ電極２１５にスルーホールを介して接続する配線２１３を形成する一方、半導体基板２１１上には、センサ電極２１５に形成される容量を検出する容量検出回路２１８を形成している。この容量検出回路２１８は、前述した配線２１３によってセンサ電極２１５に接続される。容量検出回路２１８は、センサ電極２１５毎に用意され、センサ電極２１５と認識対象（指）の一部との間に形成される容量を検出する。

【００１５】

各容量検出回路２１８の出力は、処理装置２０３に接続され、この処理装置２０３により、各センサ電極２１５に形成された容量を濃淡に変換した指紋画像データが生成される。

各容量検出回路２１８、処理装置２０３及び記憶装置２０４は、たとえばセンサ電極２１５下の半導体基板２１１上に形成する。これにより指紋センサ２０２，処理装置２０３及び記憶装置２０４をワンチップ化でき、したがって指紋認証トークン２００のワンチップ化が可能になる。なお、こうしたワンチップ化の他の例として、例えば特開２０００－２４２７７１に開示されたものがある。

【００１６】

図１３（ａ）は、容量検出回路２１８の回路図である。図１３（ａ）において

、Ｃｆは図１２におけるセンサ電極２１５と指３の皮膚との間に形成される静電容量である。容量Ｃｆを形成するセンサ電極２１５はＮchＭＯＳトランジスタＱ３ａのドレイン端子に接続されており、このトランジスタＱ３ａのソース端子は電流Ｉの電流源２１ａの入力側に接続されている。また、センサ電極２１５とトランジスタＱ３ａとの節点Ｎ１ａには、ＮchＭＯＳトランジスタ（第１の素子）Ｑ２ａのソース端子が接続されている。このトランジスタＱ２ａのドレイン端子には、ソース端子に電源電圧ＶDDが印加されたＰchＭＯＳトランジスタ（第１のスイッチ手段）Ｑ１ａのドレイン端子と、ドレイン端子に電源電圧ＶDDが印加されソース端子が抵抗Ｒａを介して接地に接続されたＮchＭＯＳトランジスタＱ４ａのゲート端子とが接続されている。このトランジスタＱ４ａのソース端子にインバータゲート４１が接続されている。

【００１７】

各トランジスタＱ１ａ，Ｑ３ａのゲート端子にはそれぞれ信号ＰＲＥ（バー），ＲＥが印加される。また、トランジスタＱ２ａのゲート端子には定電圧源からバイアス電圧ＶＧが印加される。ここで、トランジスタＱ２ａが非導通状態になるゲートーソース間のしきい値電圧をＶthとすると、ＶDD＞ＶＧ－Ｖthとなるように電圧ＶDD，ＶＧが設定される。

また、節点Ｎ１ａ，Ｎ２ａはそれぞれ寄生容量Ｃｐ１ａ，Ｃｐ２ａを有している。

【００１８】

図１３（ｂ）～図１３（ｄ）は、図１３（ａ）に示した容量検出回路２１８の動作を説明するためのタイミングチャートであり、図１３（ｂ）はトランジスタＱ１ａを制御する信号ＰＲＥ（バー）の電位変化を示し、図１３（ｃ）はトランジスタＱ３ａを制御する信号ＲＥの電位変化を示し、図１３（ｄ）は節点Ｎ１ａ，Ｎ２ａそれぞれの電位変化を示している。

最初、トランジスタＱ１ａのゲート端子にはＨｉｇｈレベル（ＶDD）の信号ＰＲＥ（バー）が与えられ、トランジスタＱ３ａのゲート端子にはＬｏｗレベル（ＧＮＤ）の信号ＲＥが与えられている。したがって、このときトランジスタＱ１ａ，Ｑ３ａはともに導通していない。

【００１９】

この状態で信号ＰＲＥ（バー）がＨｉｇｈレベルからＬｏｗレベルに変化すると、トランジスタＱ１ａが導通状態になる。このときトランジスタＱ３ａは非導通状態のままであり、信号発生回路２０は停止状態にあるから、節点Ｎ２ａの電位がＶDDにプリチャージされる。

また、トランジスタＱ２ａのゲートーソース間電圧がしきい値電圧Ｖthに達してトランジスタＱ２ａが非導通状態になるまで、節点Ｎ１ａが充電される。これにより、節点Ｎ１ａの電位がＶＧ－Ｖthにプリチャージされる。

【００２０】

プリチャージが終了した後、信号ＰＲＥ（バー）がＨｉｇｈレベルに変化すると、トランジスタＱ１ａが非導通状態になる。これと同時に信号ＲＥがＨｉｇｈレベルに変化すると、トランジスタＱ３ａが導通状態になり、信号発生回路２０が動作状態に変化する。そして、電流源２１ａにより節点Ｎ１ａに充電された電荷が引き抜かれ、節点Ｎ１ａの電位がわずかに低下すると、トランジスタＱ２ａのゲートーソース間電圧がしきい値電圧Ｖthより大きくなり、トランジスタＱ２ａが導通状態に変化する。これにより節点Ｎ２ａの電荷も引き抜かれ、節点Ｎ２ａの電位低下が開始する。

信号ＲＥをＨｉｇｈレベルにする期間をΔｔとするとΔｔ経過後の節点Ｎ１ａの電位低下ΔＶはＶDD－（ＶＧ－Ｖth）＋ＩΔｔ／（Ｃｆ＋Ｃｐ１ａ）になる。ここで、寄生容量Ｃｐ２ａは寄生容量Ｃｐ１ａに対して十分小さいとしている。

【００２１】

電流源２１ａの電流Ｉと期間Δｔと寄生容量Ｃｐ１ａ，Ｃｐ２ａは、各々一定であるから、電位低下ΔＶは、センサ電極２１５と検出対象である指の表面３との間に発生する容量の値Ｃｆによって決定される。この容量値Ｃｆはセンサ電極２１５と指の表面３との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位ΔＶの大きさが、指紋の凹凸を反映して変化する。この電位低下ΔＶが、入力信号として出力回路４０に供給されるので、出力回路４０でΔＶが入力され、指紋の凹凸を反映した信号が出力回路４０から出力される。

こうした各容量検出回路２１８の出力信号が処理装置２０３により処理され、

前述の指紋画像データとして生成される。

【００２２】

次に、上記のような指紋センサ２０２を有する指紋認証トークン１０６による利用者本人の認証動作を図９のフローチャートを参照して説明する。

利用者が指紋認証トークン１０６の指紋センサ２０２上に自身の指をのせる（と（ステップＳ４１）、指紋認証トークン１０６の処理装置２０３は、指紋センサ２０２により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップＳ４２）。ここで、指紋認証トークン１０６の記憶装置２０４には、予め指紋センサ２０２により検出され処理装置２０３により処理された利用者自身の指紋画像データ中の特徴部分を示す照合情報が登録されており、処理装置２０３は、記憶装置２０４に保存されているこの登録情報と、ステップＳ４２で抽出した照合情報とを比較する（ステップＳ４３）。そして、双方の照合情報が一致してステップＳ４４の「照合情報が一致？」の判定がＹＥＳとなると、処理装置２０３は、利用者本人であることを認証する（ステップＳ４５）。

【００２３】

次に、以上のような指紋認証トークン１０６を用いた本システムの動作を図５～図８のフローチャートを参照して説明する。

（第１の実施の形態）

まず、図５及び図６のフローチャートを用いて本システムの第１の実施の形態の動作を説明する。

利用者が例えばコンサート会場でのコンサートを聴く場合、予めチケットを購入することになるが、この場合利用者は図５のステップＳ１で例えばチケット販売店や自宅のクレードル１０１に自身の指紋認証トークン１０６を挿入し、チケット販売店にチケット代金の支払いを行う（ステップＳ２）。

【００２４】

すると、クレードル１０１はパスワードを発行し指紋認証トークン１０６に送信する（ステップＳ３）。指紋認証トークン１０６の処理装置２０３はこのパスワードを受信すると記憶装置２０４に記憶する（ステップＳ４）。また、クレー

ドル１０６は、発行したパスワードをネットワーク１０５を介してデータベース１０２に送信し、データベース１０２に保存させる（ステップＳ５）。

【００２５】

こうして、チケット代金を支払いパスワードが記録された指紋認証トークン１０６を所持した利用者は、コンサート開演の当日そのコンサート会場に赴くことになる。なお、この場合、利用者は前述の指紋認証トークン１０６に図３または図４に示すアダプタを付加した無線通信ユニット１０７または赤外線通信ユニット１０８として所持する。

【００２６】

図６のフローチャートはこのときのシステムの動作を示すフローチャートである。

コンサート会場の入場ゲート１０４はステップＳ１１のように閉じたままの状態となっている。ここで、利用者は所持した無線通信ユニット１０７または赤外線通信ユニット１０８を用いて自身の指を指紋センサ２０２に押捺することにより本人認証を行う（ステップＳ１２）。この場合、無線通信ユニット１０７または赤外線通信ユニット１０８の処理装置２０３は、前述した図９のフローチャートのステップ４３に示すように、指紋センサ２０２により検出された指紋と記憶装置２０４の登録指紋データとを比較照合する。そして、双方の指紋が一致してステップＳ１３の「本人であるか？」の判定がＹＥＳとなると、無線通信ユニット１０７または赤外線通信ユニット１０８は、チケット購入時に指紋認証トークン１０６に保存したパスワードを無線信号または赤外線信号に変換して、ゲート１０４近傍の無線／赤外線信号受信装置１０９へ送信する（ステップＳ１４）。この無線信号または赤外線信号によるパスワードは無線／赤外線信号受信装置１０９により受信される。

【００２７】

ゲートコントローラ１０３は、無線／赤外線信号受信装置１０９を介してこのパスワードを取得すると（ステップＳ１５）、取得したパスワードとデータベース１０２に保存されているパスワードと比較する（ステップＳ１６）。そして、双方のパスワードが一致しステップＳ１７の判定がＹＥＳとなると、ゲート１０

４を開放する（ステップＳ１８）。これにより、利用者はコンサート会場へ入場することができる。なお、競技場で試合を観戦する場合も同様である。

【００２８】

このように、例えばコンサートのチケット購入時に利用者がその代金を支払うと、データベース１０２及び利用者の指紋認証トークン１０６にパスワードを記憶するとともに、コンサート会場の入場時に利用者が所持した指紋認証トークン１０６により利用者本人の確認を行い、利用者本人であることが認証されて指紋認証トークン１０６から入場ゲート１０４近傍の無線／赤外線信号受信装置１０９へパスワードが送信されると、このパスワードを無線／赤外線信号受信装置１０９を介して受信したゲートコントローラ１０３は、データベース１０２のパスワードとの比較を行い双方のパスワードが一致すると入場ゲート１０４を開放するようにしたものである。この結果、コンサート会場や競技場への入場時にはチケットが不要になり、したがって、チケットのチェック要員を無くすことができるとともに、利用者はコンサート会場や競技場へ速やかに入場できる。また、利用者の指紋認証トークン１０６が盗難され、その指紋認証トークン１０６を利用して第三者が不正に入場しようとしても、利用者の指紋画像と異なることから第三者による不正入場を阻止できる。また、指紋認証トークン１０６を紛失した場合、新たな指紋認証トークンを用い図５の各ステップに示す手順と同様の手順を行うことによりチケットの再発行を行うことができる。

【００２９】

（第２の実施の形態）

次に、図７及び図８を参照して、本システムの第２の実施の形態の動作を説明する。

利用者がコンサート会場でコンサートを聴く場合、予め利用者は図７のステップＳ２１でチケット販売店や自宅のクレードル１０１に自身の指紋認証トークン１０６を挿入し、チケット販売店にチケット代金の支払いを行う（ステップＳ２２）。

【００３０】

すると、指紋認証トークン１０６は、予め記憶装置２０４に付与されている識

別番号をクレードル１０１に送信する（ステップＳ２３）。クレードル１０１はこの識別番号を受信すると、受信した識別番号をネットワーク１０５を介してデータベース１０２に送信し、データベース１０２に保存させる（ステップＳ２４）。

【００３１】

こうして、チケット代金を支払うことにより、自身の識別番号をデータベース１０２に保存した指紋認証トークン１０６を所持した利用者は、コンサート開演の当日そのコンサート会場に赴くことになる。なお、この場合、利用者は前述の指紋認証トークン１０６に図３または図４に示すアダプタを付加した無線通信ユニット１０７または赤外線通信ユニット１０８として所持する。

【００３２】

図８のフローチャートはこのときのシステムの動作を示すフローチャートである。

コンサート会場の入場ゲート１０４はステップＳ３１のように閉じたままの状態となっている。ここで、利用者は所持した無線通信ユニット１０７または赤外線通信ユニット１０８を用いて自身の指を指紋センサ２０２に押捺することにより本人認証を行う（ステップＳ３２）。この場合、無線通信ユニット１０７または赤外線通信ユニット１０８の処理装置２０３は、前述した図９のフローチャートのステップ４３に示すように、指紋センサ２０２により検出された指紋と記憶装置２０４の登録指紋データとを比較照合する。そして、双方の指紋が一致してステップＳ３３の「本人であるか？」の判定がＹＥＳとなると、無線通信ユニット１０７または赤外線通信ユニット１０８は、予め指紋認証トークン１０６に付与されている識別番号を無線信号または赤外線信号に変換して、ゲート１０４近傍の無線／赤外線信号受信装置１０９へ送信する（ステップＳ３４）。この無線信号または赤外線信号による識別番号は無線／赤外線信号受信装置１０９により受信される。

【００３３】

ゲートコントローラ１０３は、無線／赤外線信号受信装置１０９を介してこの識別番号を取得すると（ステップＳ３５）、取得した識別番号とデータベース１

０２に保存されている識別番号と比較する（ステップＳ３６）。そして、双方の識別番号が一致しステップＳ３７の判定がＹＥＳとなると、ゲート１０４を開放する（ステップＳ３８）。これにより、利用者はコンサート会場へ入場することができる。なお、競技場で試合を観戦する場合も同様である。

【００３４】

このように、例えばコンサートのチケット購入時に利用者がその代金を支払うと、利用者の指紋認証トークン１０６に付与されている識別番号をデータベース１０２に記憶するとともに、コンサート会場の入場時に利用者が所持した指紋認証トークン１０６により利用者本人の確認を行い、利用者本人であることが認証されて指紋認証トークン１０６から入場ゲート１０４近傍の無線／赤外線信号受信装置１０９へ識別番号が送信されると、この識別番号を無線／赤外線信号受信装置１０９を介して受信したゲートコントローラ１０３は、データベース１０２の識別番号との比較を行い双方の識別番号が一致すると入場ゲート１０４を開放するようにしたものである。この結果、コンサート会場や競技場への入場時にはチケットが不要になり、したがって、チケットのチェック要員を無くすことができるとともに、コンサート会場や競技場へ速やかに入場できる。また、利用者の指紋認証トークン１０６が盗難され、その指紋認証トークン１０６を利用して第三者が不正に入場しようとしても、利用者の指紋画像と異なることから第三者による不正入場を阻止できる。また、指紋認証トークン１０６を紛失した場合、新たな指紋認証トークンを用い図７の各ステップに示す手順を再度行うことによりチケットの再発行を行うことができる。

【００３５】

なお、本実施の形態では、パスワードまたは識別番号を用いてゲート１０４を開放するようにしたが、ワンタイムパスワードを用いるようにしても良い。

また、本実施の形態では、利用者の入場ゲート４の通過時に無線通信ユニット１０７または赤外線通信ユニット１０８から無線信号または赤外線信号によるパスワードや識別番号等を送信するようにしたが、ゲート１０４の近傍にゲートコントローラ１０３に接続され指紋認証トークン１０６が挿入可能なクレードルを設ければ、指紋認証トークン１０６のみによりゲート１０４を通過できる。

また、本実施の形態では、利用者のチケット購入時にチケット販売店や自宅のクレードル１０１に指紋認証トークン１０６を挿入するようにしているが、チケット販売店や自宅のクレードル１０１に無線／赤外線信号受信装置を設ければ、無線通信ユニット１０７または赤外線通信ユニット１０８によりチケットを購入することができる。

【００３６】

また、本実施の形態では、無線通信ユニットとして図３に示すような構造の無線通信ユニット１０７を用いるようにしたが、図１０に示すような腕時計型の構造を有するものや、ブレスレット型、或いはペンダント型の構造を有するものであっても良い。なお、赤外線通信ユニット１０８の構造についても前述した無線通信ユニットの構造と同様の構造を有するものであっても良い。

【００３７】

また、本実施の形態では、図１に示すようにデータベース１０２とゲートコントローラ１０３が専用線で結ばれた例を説明したが、図１１に示すようにデータベース１０２とゲートコントローラ１０３をネットワーク１０５を介して接続するようにしても良い。

ここで、データベース１０２は、図１及び図１２には示されていないが、サーバ機能を含むものである。このサーバ機能は、ネットワーク１０５に接続されたものであれば、データベース１０２と一体でなくても良く、クレードル１０１やゲートコントローラ１０３が代替しても良い。さらに、１つのサーバでシステム全体の制御を行わずに、クレードル１０１とゲートコントローラ１０３とで分散して処理するようにしても良い。

【００３８】

また、本実施の形態では、指紋認証トークン１０６内の指紋センサ２０２，処理装置２０３，記憶装置２０４をワンチップで構成した第１の構成例について説明したが、上記第１の構成例の他に、指紋センサ２０２をワンチップ化し、このワンチップ指紋センサ２０２に、バスを介して処理装置２０３を接続し、さらに処理装置２０３にバスを介して記憶装置２０４を接続する第２の構成例がある。さらに、指紋センサ２０２と処理装置２０３をワンチップ化し、このワンチップ

化された処理装置２０３にバスを介して記憶装置２０４を接続する第３の構成例がある。

【００３９】

また、指紋認証トークン１０６とクレードル１０１間、クレードル１０１とデータベース１０２間、データベース１０２とゲートコントローラ１０３間、及び無線通信ユニット１０７または赤外線通信ユニット１０８と無線／赤外線信号受信装置１０９間で、それぞれ送受される信号を送信側で暗号化し、受信側でその暗号化データを復号化することにより、システムのセキュリティを向上させることができる。

また、本実施の形態では、指紋の認証に基づいてゲート１０４の開閉を制御するようにしたが、指の大きさ、手形、静脈パターン、人相、虹彩及び声紋などの利用者固有の生体情報や、利用者のサイン（筆跡）等により利用者本人であることを認証してゲート１０４を開放するようにしても良い。

【００４０】

図１４は、前述の指紋認証トークン１０６を含む利用者固有の生体情報や利用者のサイン等により認証を行う認証トークン３００と、認証トークン３００の認証を利用してゲート１０４の開閉を制御する前述のゲートコントローラ１０３を含む利用機器４００とからなる認証システムの構成を示すブロック図である。

この認証システムでは、ユーザ固有の生体情報として指紋を用いる場合を例として説明する。

【００４１】

認証トークン３００には、指紋（生体情報）を読み取るセンサ３１１（図２の指紋センサ２０２に対応）、ユーザ本人の登録指紋データ３１２Ａやユーザ情報３１２Ｂを記憶する記憶回路３１２（図２の記憶装置２０４に対応）、センサ３１１での読み取り結果を示すセンシングデータ３１１Ａを、記憶回路３１２に記憶されている登録指紋データ３１２Ａを用いて照合する照合回路３１３（図２の処理装置２０３に対応）、この照合回路３１３での照合結果を含む認証データ３１３Ａを通信データ３０１Ａとして認証トークン３００の外部へ送信する通信回路３１４（図２の処理装置２０３に対応）が設けられており、これら回路部を一

体として形成する認証トークン３００が利用機器４００に対して着脱自在に接続される。

利用機器４００には、認証トークン３００からの通信データ３０１Ａを受信する通信回路４２１と、受信した通信データ３０１Ａに含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置４２２とが設けられている。

【００４２】

次に、図１４に示す認証システムの動作について説明する。

ユーザは事前に、自分の所持する認証トークン３００の記憶回路３１２に、自分の登録指紋データ３１２Ａやサービスを利用するためのパスワードや個人情報などからなるユーザ情報３１２Ｂを記憶させておく。

利用機器４００を利用する際、まずユーザは自分の認証トークン３００を利用機器４００へ接続し、指をそのセンサ３１１へ置く。これにより認証トークン３００のセンサ３１１でユーザの指紋が読み取られセンシングデータ３１１Ａとして出力される。このセンシングデータ３１１Ａは照合回路３１３において記憶回路３１２の登録指紋データ３１２Ａを用いて照合される。そして、その照合結果を含む認証データ３１３Ａが出力される。このとき照合回路３１３は、予め記憶回路３１２に格納されているユーザＩＤ、パスワード、個人情報などのユーザ情報３１２Ｂを読み出し、認証データ３１３Ａへ含めて出力する。なお、認証トークン３００から出力する情報は、これらの情報の中から選択することができ、本発明のゲート開閉システムでは、パスワードまたは識別情報のみでも良いし、必要に応じてその他の情報を付加しても良い。

【００４３】

通信回路３１４では、照合回路３１３からの認証データ３１３Ａを通信データ３０１Ａとして利用機器４００へ送信する。

利用機器４００の通信回路４２１では、認証トークン３００の通信回路３１４から送信された通信データ３０１Ａを受信し、認証データ３１３Ａと同じ内容の認証データ４２１Ａとして出力する。処理装置４２２では、この認証データ４２１Ａを受け取ってその認証データ４２１Ａに含まれる照合結果を参照する。そし

て、その照合結果が一致を示す場合、処理装置４２２においてユーザの所望する所定の処理が実行される。

【００４４】

このように、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ３１１と、ユーザの指紋を照合するための登録指紋データ３１２Ａが予め格納されている記憶回路３１２と、この記憶回路３１２に記憶されている登録指紋データ３１２Ａを用いてセンサ３１１からのセンシングデータ３１１Ａを照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路３１３と、この照合回路３１３からの認証データを通信データ３０１Ａとして利用機器４００へ送信する通信回路３１４とを、認証トークン３００として一体として形成したものである。

【００４５】

そして、認証に応じて所定の処理を行う利用機器４００をユーザが利用する場合には、認証トークン３００をその利用機器４００へ接続し、その認証トークン３００でユーザの生体情報に基づきユーザ認証を行い、利用機器４００へ通知するようにしたものである。

また、利用機器４００に、認証トークン３００から送信された通信データ３０１Ａを受信し認証データ４２１Ａとして出力する通信回路４２１と、この通信回路４２１からの認証データ４２１Ａに含まれる照合結果に基づき所定の処理を行う処理装置４２２とを設け、この利用機器４００とは独立した各ユーザが個々の持つ認証トークン３００での認証結果に基づき所定の処理を行うようにしたものである。

【００４６】

したがって、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及

せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。なお、認証トークン３００については、センサ、記憶回路および照合回路などを1チップの半導体装置として形成する技術（例えば、特開２０００－２４２７７１号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

【００４７】

さらに、記憶回路３１２にユーザＩＤやパスワードさらには個人情報などのユーザ情報３１２Ｂを予め記憶しておき、これらを認証データ３１３Ａに含めて利用機器４００へ送信するようにしたので、利用機器４００の処理装置４２２において、その認証データに含まれるユーザ情報３１２Ｂ、例えばユーザＩＤやパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報３１２Ｂの個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

【００４８】

なお、利用機器４００に図示しない乱数発生回路及び復号回路を設け、かつ認証トークン３００に図示しない暗号化回路を設けて、利用機器４００と認証トークン３００間で通信されるデータの暗号化することにより、セキュリティの向上を図ることができる。

【００４９】

即ち、利用機器４００は、認証トークン３００側からのアクセス時に乱数発生回路により乱数を発生させてこの乱数を通信回路４２１から認証トークン３００へ送信して暗号化回路に記憶させる一方、認証トークン３００の暗号化回路は照合回路３１３から出力された認証データ３１３Ａと、記憶した乱数との和を演算してその演算結果を、予め記憶回路３１２に記憶してある共通鍵により暗号化して暗号化データとして利用機器４００側へ送信する。利用機器４００では、通信回路４２１により受信したこの暗号化データを復号回路が共通鍵を用いて復号化

するとともに復号化したデータから乱数発生回路が発生した前記乱数を減算することにより認証データ４２１Ａとして処理回路４２２へ出力する。なお、上記の例では、認証トークン３００及び利用機器４００の双方に共通鍵を持たせて、それぞれ暗号化及び復号化を行わせているが、認証トークン３００に秘密鍵を、利用機器４００に公開鍵を持たせてそれぞれ暗号化処理及び復号化処理を行わせることもできる。

【００５０】

次に、図１５を参照して、本認証システムの第２の構成例について説明する。図１５は、図１４に示す第１の構成例のうち、認証トークン３００の出力段にデータ変換モジュール３３０を付加したものである。

このデータ変換モジュール３３０には、認証トークン３００の通信回路３１４から出力された通信データを、利用機器４００で受信・解読可能なデータ形式へ変換するプロトコル変換回路３３１が設けられている。

【００５１】

このように、認証トークン３００に着脱自在に取り付けられるデータ変換モジュール３３０を介して、所望の利用機器４００と認証トークン３００とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが１つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。

以上では、データ変換モジュール３３０を認証トークン３００に対して着脱自在に取り付ける場合を例として説明したが、認証トークン３００内部にプロトコル変換回路３３１を設けてもよく、さらにコンパクトに構成できる。

【００５２】

次に、図１６を参照して、本認証システムの第３の構成例について説明する。図１６は、図１４に示す第１の構成例のうち、認証トークン３００の出力段に無線モジュール３４０を付加したもので、この無線モジュール３４０は前述の無線通信ユニット１０７に相当するものである。

この無線モジュール３４０には、認証トークン３００の通信回路３１４から出力された通信データを、利用機器４００で受信・解読可能なデータ形式へ変換するプロトコル変換装置３４１と、このプロトコル変換装置３４１からの通信データを無線区間を介して利用機器４００へ送信する無線回路３４２とが設けられている。この場合、利用機器４００側にも無線回路４２３を設ける必要がある。

【００５３】

このように、認証トークン３００に着脱自在に取り付けられる無線モジュール３４０を用いて、所望の利用機器４００と認証トークン３００とを接続するようにしたので、ユーザは、認証トークン３００を利用機器４００に直接接続することなく、例えば自分の手元で認証トークン３００を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器４００に対して認証トークン３００を接続する作業や、利用機器４００に接続されている状態の認証トークン３００を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

【００５４】

なお、利用機器４００と認証トークン３００の通信プロトコルが同一の場合は、無線モジュール３４０のプロトコル変換回路３４１を省略することも可能である。また、無線回路３４２の代わりに、前述の赤外線通信ユニット１０８のような赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール３４０を認証トークン３００に対して着脱自在に取り付ける場合を例として説明したが、認証トークン３００内部に無線回路３４２やプロトコル変換回路３４１を設けてもよく、さらにコンパクトに構成できる。

【００５５】

【発明の効果】

以上説明したように本発明によれば、会場の入場ゲートを開閉するゲート開閉システムにおいて、利用者の生体情報に基づき利用者本人を認証する認証トークンと、利用者が前記会場の入場料の前払いを行うと利用者の識別情報が記憶されるデータベースとを設け、利用者の前記会場への入場時に認証トークンにより利

用者が本人であると認証されこの認証トークンに予め記憶されている利用者の識別情報が認証トークンから出力されると、この識別情報を受信するとともに受信した識別情報がデータベース内に記憶されている場合は入場ゲートを開放するようにしたので、利用者がコンサート会場や競技場への入場時にはチケットが不要になり、したがって、チケットのチェック要員を無くすことができるとともに、利用者はコンサート会場や競技場へ速やかに入場できる。また、利用者の認証トークンが盗難され、その認証トークンを利用して第三者が不正に入場しようとしても、利用者の生体情報と異なることから第三者による不正入場を阻止でき、したがって利用者の的確な入場管理を行うことができる。

【図面の簡単な説明】

【図１】　本発明に係るゲート開閉システムの構成を示すブロック図である。

【図２】　ゲート開閉システムに用いられる指紋認証トークンの外観を示す図（図２（ａ））及びその構成を示すブロック図（図２（ｂ））である。

【図３】　ゲート開閉システムに用いられる無線通信ユニットの外観を示す図（図３（ａ））及びその構成を示すブロック図（図３（ｂ））である。

【図４】　ゲート開閉システムに用いられる赤外線通信ユニットの外観を示す図（図４（ａ））及びその構成を示すブロック図（図４（ｂ））である。

【図５】　ゲート開閉システムの第１の実施の形態の動作を示すフローチャートである。

【図６】　ゲート開閉システムの第１の実施の形態の動作を示すフローチャートである。

【図７】　ゲート開閉システムの第２の実施の形態の動作を示すフローチャートである。

【図８】　ゲート開閉システムの第２の実施の形態の動作を示すフローチャートである。

【図９】　指紋認証トークンにおける利用者認証動作を示すフローチャートである。

【図１０】　ゲート開閉システムに用いられる他の通信ユニットの例を示す

図である。

【図１１】　ゲート開閉システムの他の構成を示すブロック図である。

【図１２】　前記指紋認証トークンを構成する指紋センサの詳細構成を示す図である。

【図１３】　前記指紋センサ内の容量検出回路の回路図及び前記容量検出回路の各部の動作タイミングを示すタイムチャートである。

【図１４】　認証トークンおよび利用機器からなる認証システムの第１の構成例を示すブロック図である。

【図１５】　認証トークンおよび利用機器からなる認証システムの第２の構成例を示すブロック図である。

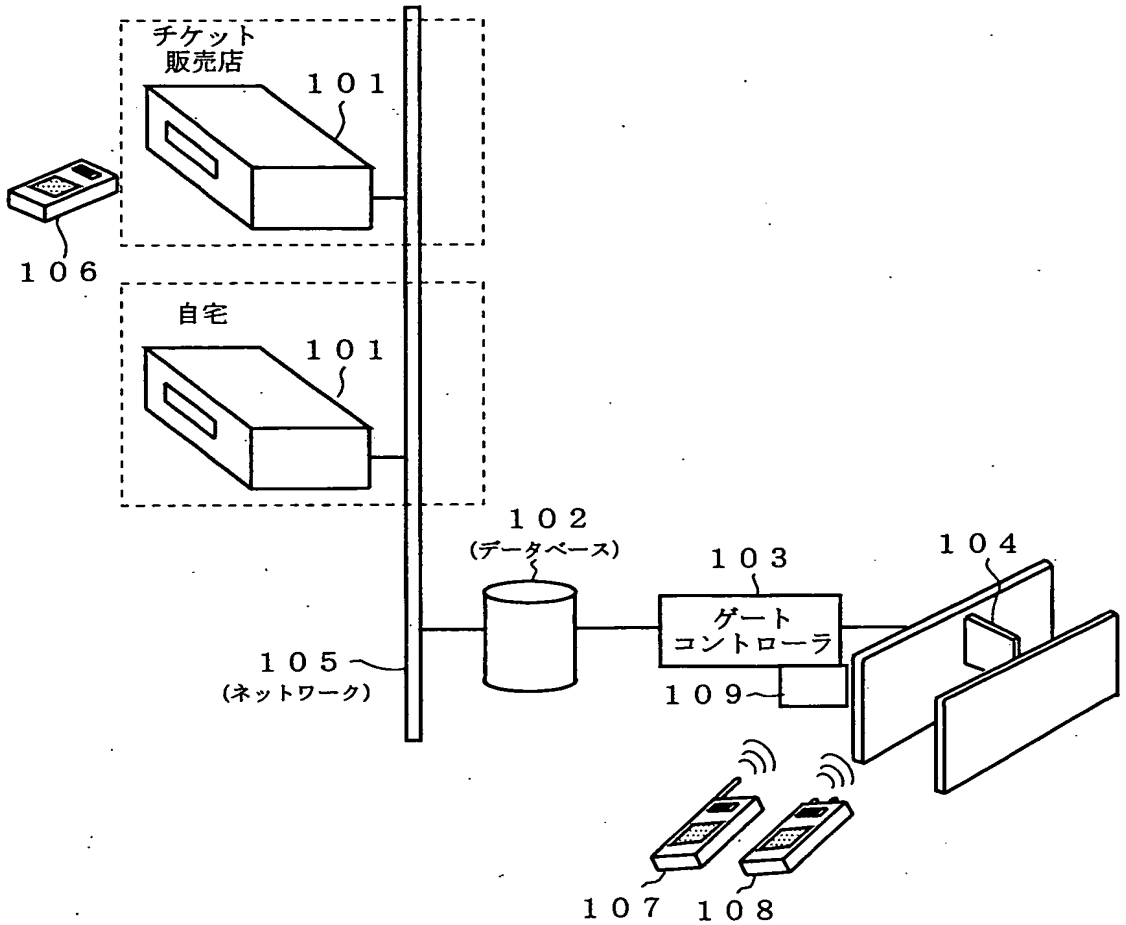
【図１６】　認証トークンおよび利用機器からなる認証システムの第３の構成例を示すブロック図である。

【符号の説明】

１０１…クレードル、１０２…データベース、１０３…ゲートコントローラ、１０４…ゲート、１０５…ネットワーク、１０６…指紋認証トークン、１０７…無線通信ユニット、１０８…赤外線通信ユニット、１０９…無線／赤外線信号受信装置、２０２…指紋センサ、２０３…処理装置、２０４…記憶装置、２１１…半導体基板、２１２…下層絶縁膜、２１３…配線、２１４…層間絶縁膜、２１５…センサ電極、２１７…パシベーション膜、２１８…容量検出回路、３０２…アンテナ、３０３…無線信号発生回路、４０２…赤外線光源、４０３…赤外線信号発生回路。

【書類名】　　図面

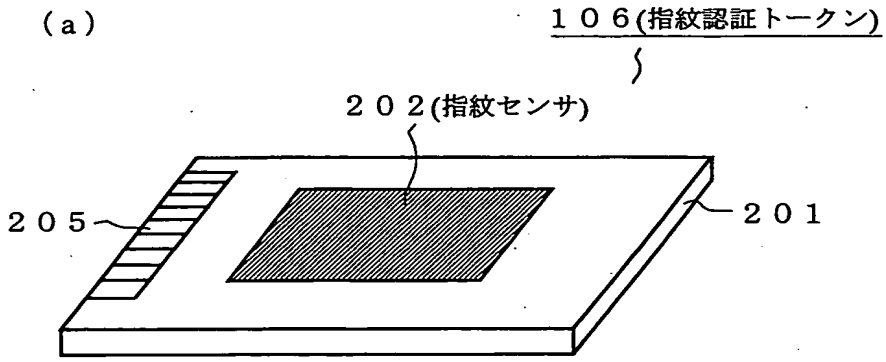
【図１】



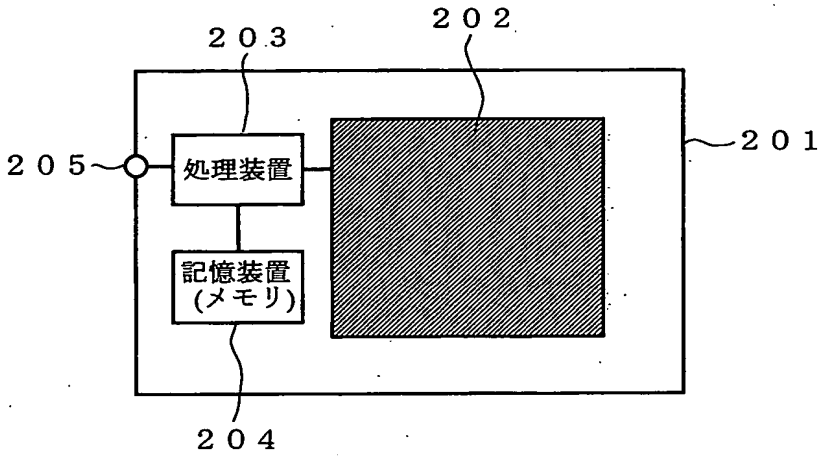
（注）１０９：無線／赤外線信号受信装置

【図２】

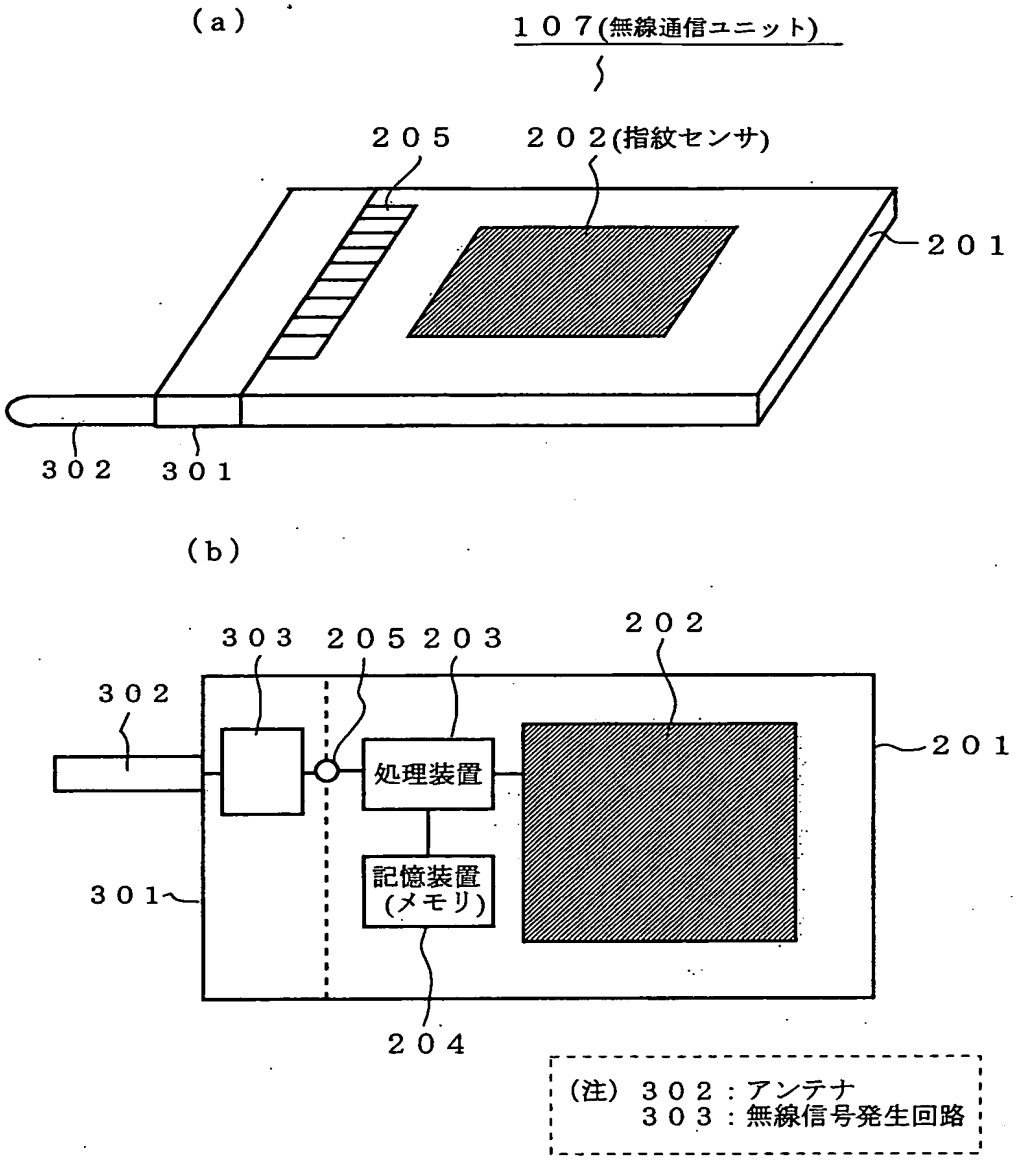
（ａ）


１０６(指紋認証トークン)
２０２(指紋センサ)
２０５
２０１

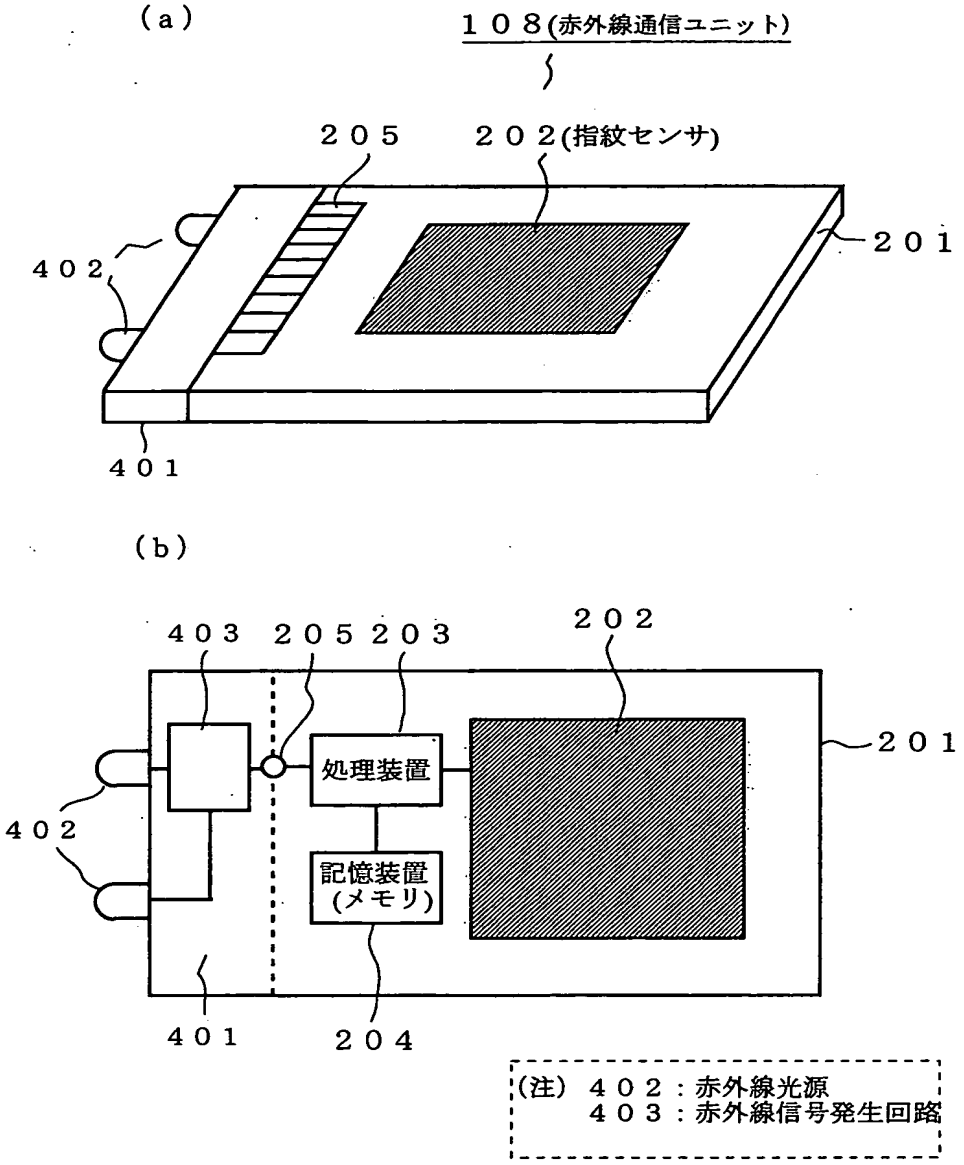
（ｂ）


２０３
２０２
２０５
処理装置
２０１
記憶装置
(メモリ)
２０４

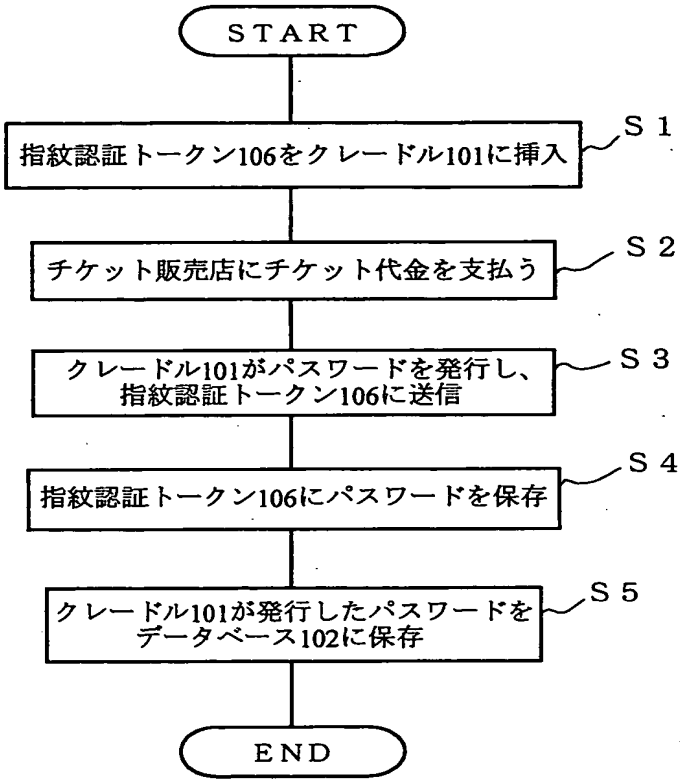
【図３】


（ａ）
１０７(無線通信ユニット)
２０５
２０２(指紋センサ)
２０１
３０２
３０１
（ｂ）
３０３
２０５
２０３
２０２
３０２
２０１
処理装置
記憶装置
(メモリ)
３０１
２０４
（注）３０２：アンテナ
３０３：無線信号発生回路

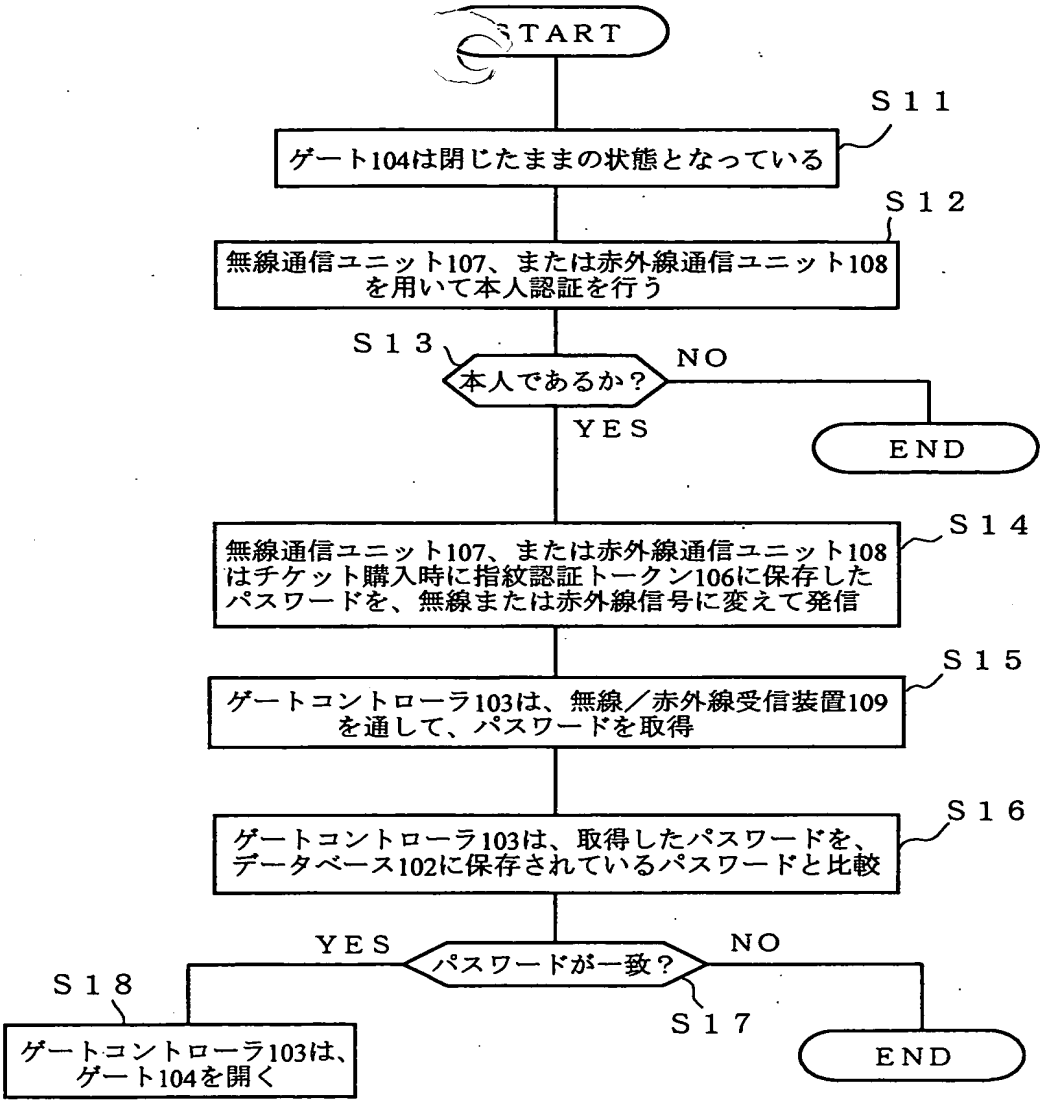
【図４】


（ａ）
１０８(赤外線通信ユニット)
２０５
２０２(指紋センサ)
２０１
４０２
４０１
（ｂ）
４０３
２０５
２０３
２０２
２０１
処理装置
４０２
記憶装置
(メモリ)
４０１
２０４
(注) ４０２：赤外線光源
４０３：赤外線信号発生回路

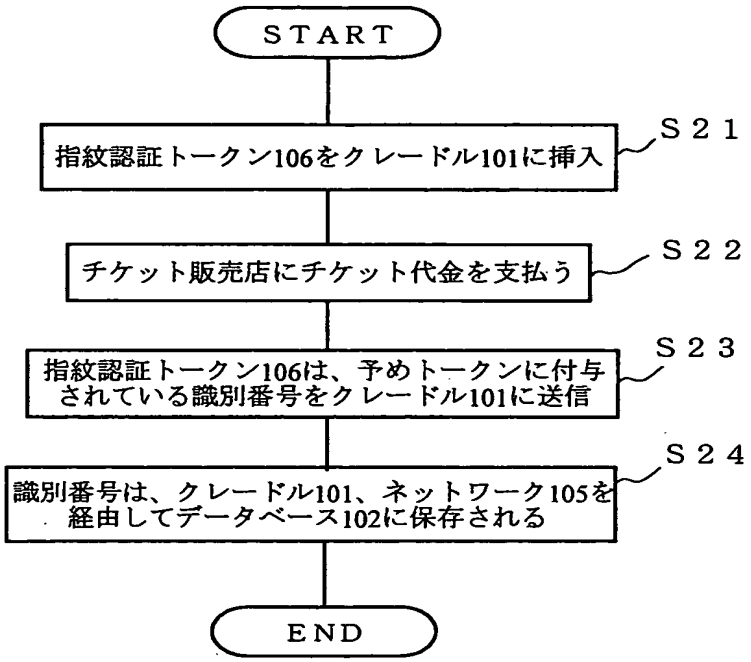
【図５】


START
指紋認証トークン106をクレードル101に挿入
S１
チケット販売店にチケット代金を支払う
S２
クレードル101がパスワードを発行し、
指紋認証トークン106に送信
S３
指紋認証トークン106にパスワードを保存
S４
クレードル101が発行したパスワードを
データベース102に保存
S５
END

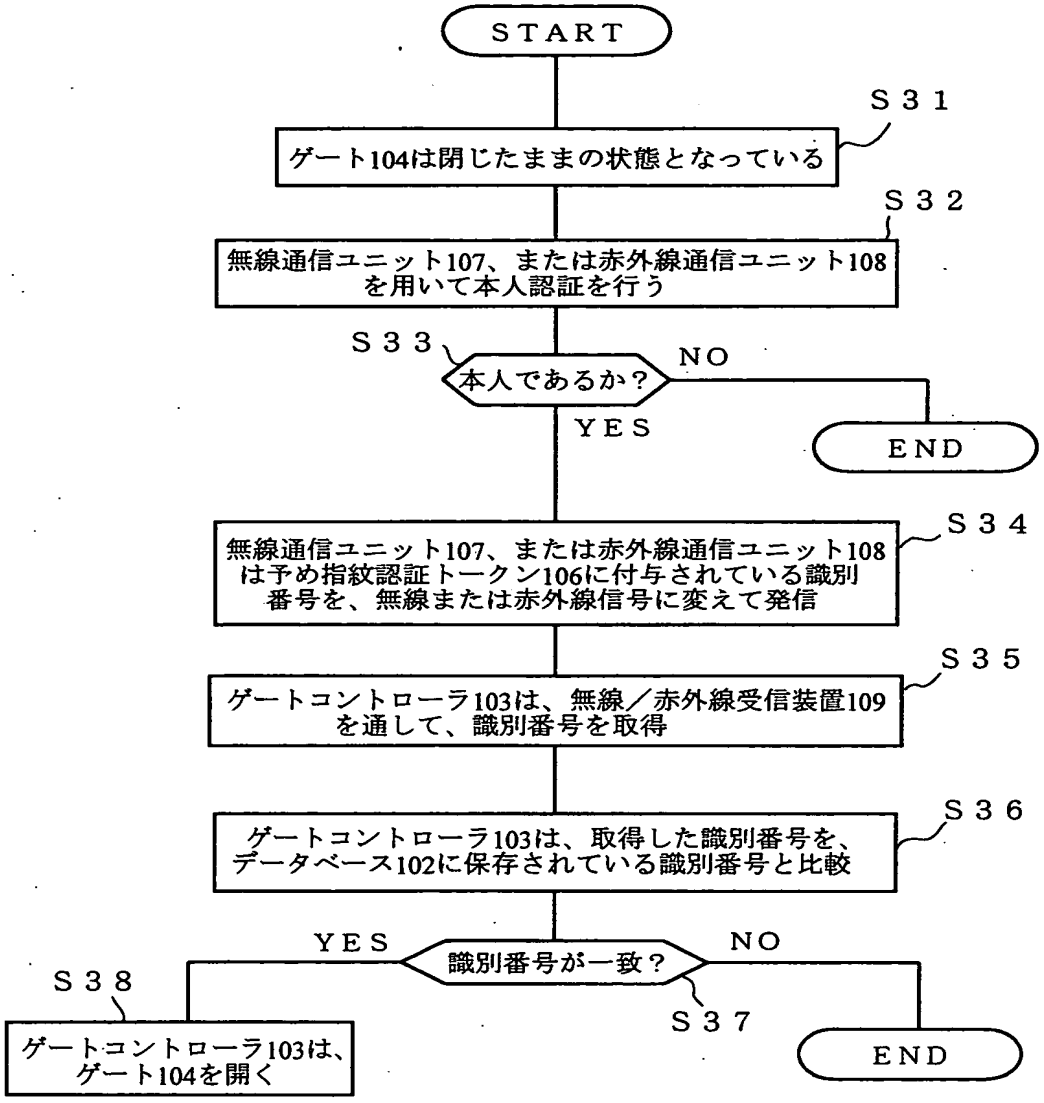
【図６】


START
S１１
ゲート104は閉じたままの状態となっている
S１２
無線通信ユニット107、または赤外線通信ユニット108
を用いて本人認証を行う
S１３
本人であるか？
NO
YES
END
S１４
無線通信ユニット107、または赤外線通信ユニット108
はチケット購入時に指紋認証トークン106に保存した
パスワードを、無線または赤外線信号に変えて発信
S１５
ゲートコントローラ103は、無線／赤外線受信装置109
を通して、パスワードを取得
S１６
ゲートコントローラ103は、取得したパスワードを、
データベース102に保存されているパスワードと比較
YES
パスワードが一致？
NO
S１８
S１７
ゲートコントローラ103は、
ゲート104を開く
END

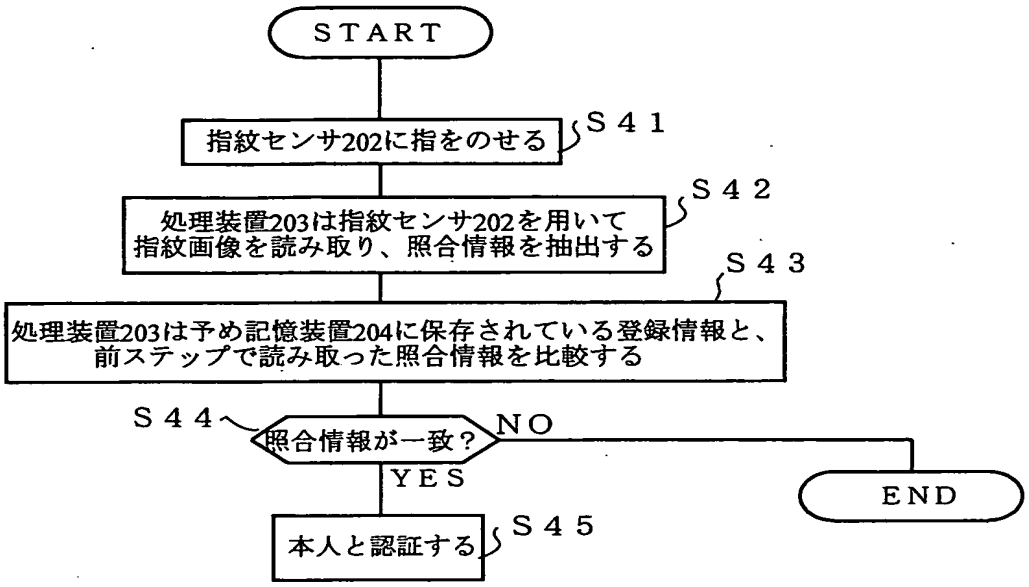
【図７】


START
指紋認証トークン106をクレードル101に挿入
Ｓ２１
チケット販売店にチケット代金を支払う
Ｓ２２
指紋認証トークン106は、予めトークンに付与されている識別番号をクレードル101に送信
Ｓ２３
識別番号は、クレードル101、ネットワーク105を経由してデータベース102に保存される
Ｓ２４
END

【図８】

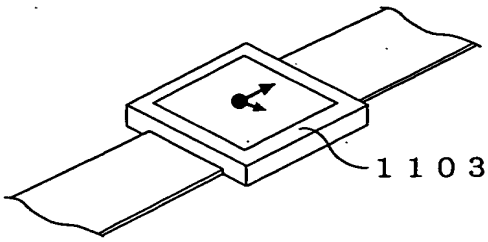

START
S３１
ゲート104は閉じたままの状態となっている
S３２
無線通信ユニット107、または赤外線通信ユニット108を用いて本人認証を行う
S３３
本人であるか？
NO
YES
END
無線通信ユニット107、または赤外線通信ユニット108は予め指紋認証トークン106に付与されている識別番号を、無線または赤外線信号に変えて発信
S３４
ゲートコントローラ103は、無線／赤外線受信装置109を通して、識別番号を取得
S３５
ゲートコントローラ103は、取得した識別番号を、データベース102に保存されている識別番号と比較
S３６
YES
識別番号が一致？
NO
S３８
S３７
ゲートコントローラ103は、ゲート104を開く
END

【図９】

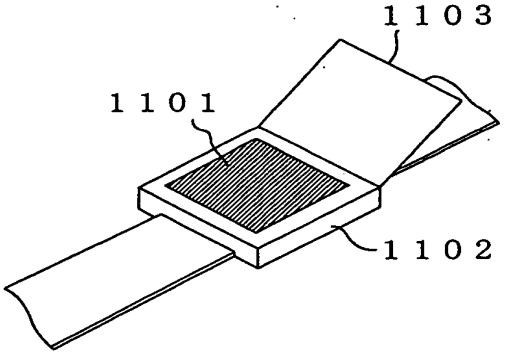

START
指紋センサ202に指をのせる
Ｓ４１
処理装置203は指紋センサ202を用いて
指紋画像を読み取り、照合情報を抽出する
Ｓ４２
処理装置203は予め記憶装置204に保存されている登録情報と、
前ステップで読み取った照合情報を比較する
Ｓ４３
Ｓ４４
照合情報が一致？
NO
YES
END
本人と認証する
Ｓ４５

【図１０】

（ａ）通常時

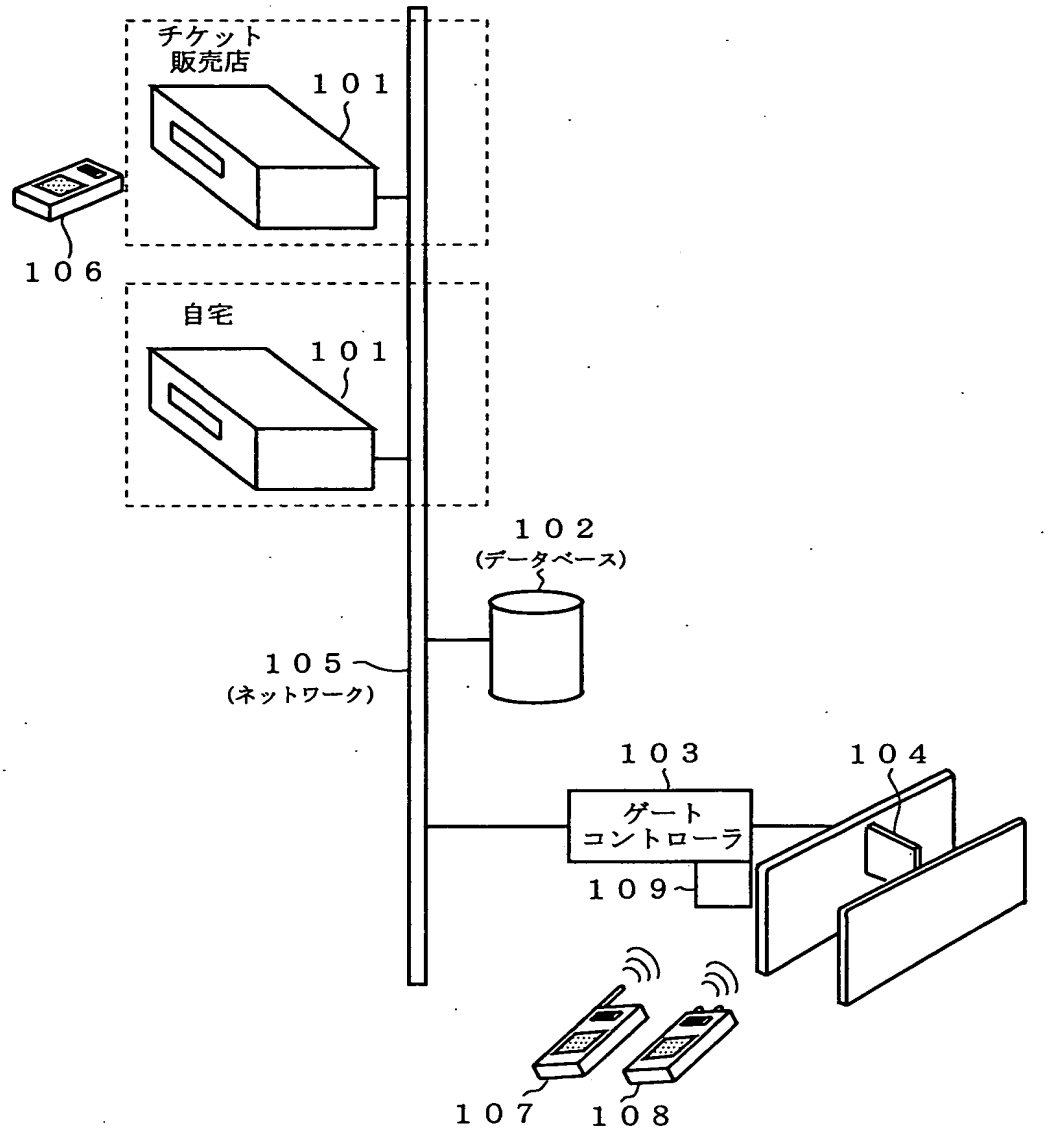


（ｂ）指紋認証時



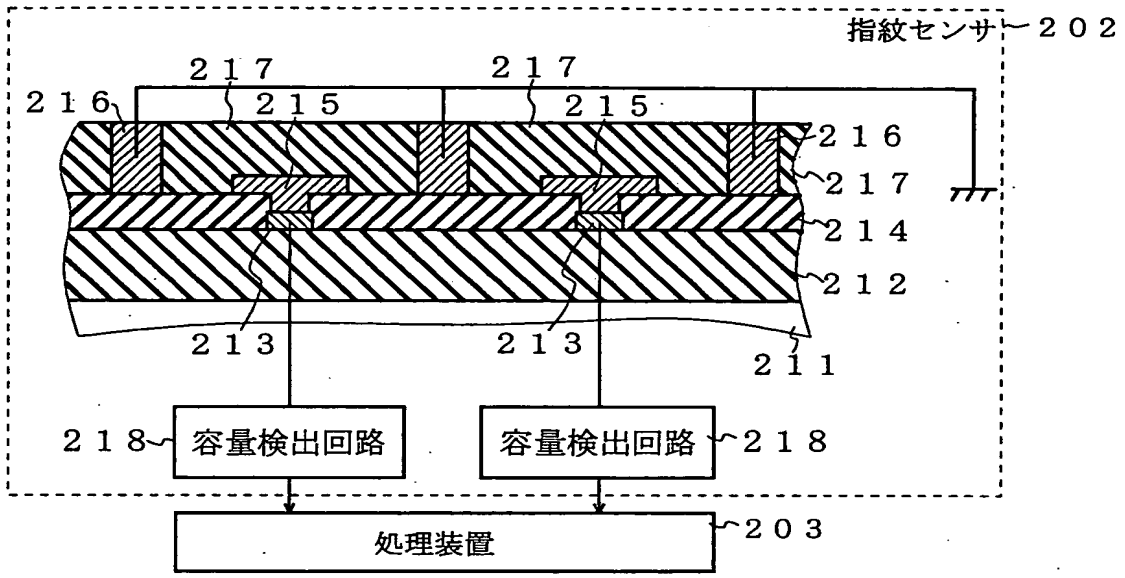
（注）1101：指紋センサ
1102：アンテナ
1103：時刻表示部

【図１１】

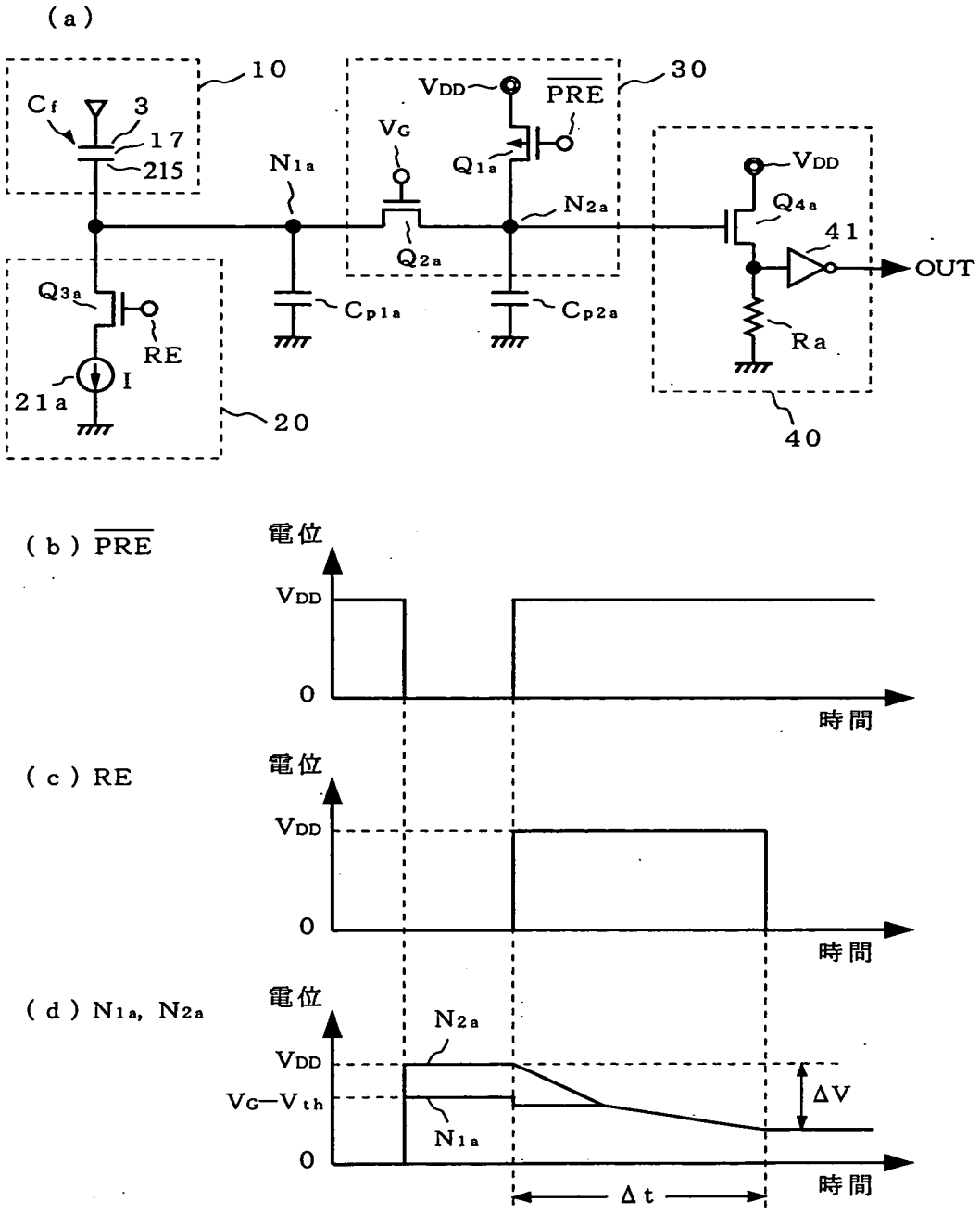


（注）１０９：無線／赤外線信号受信装置

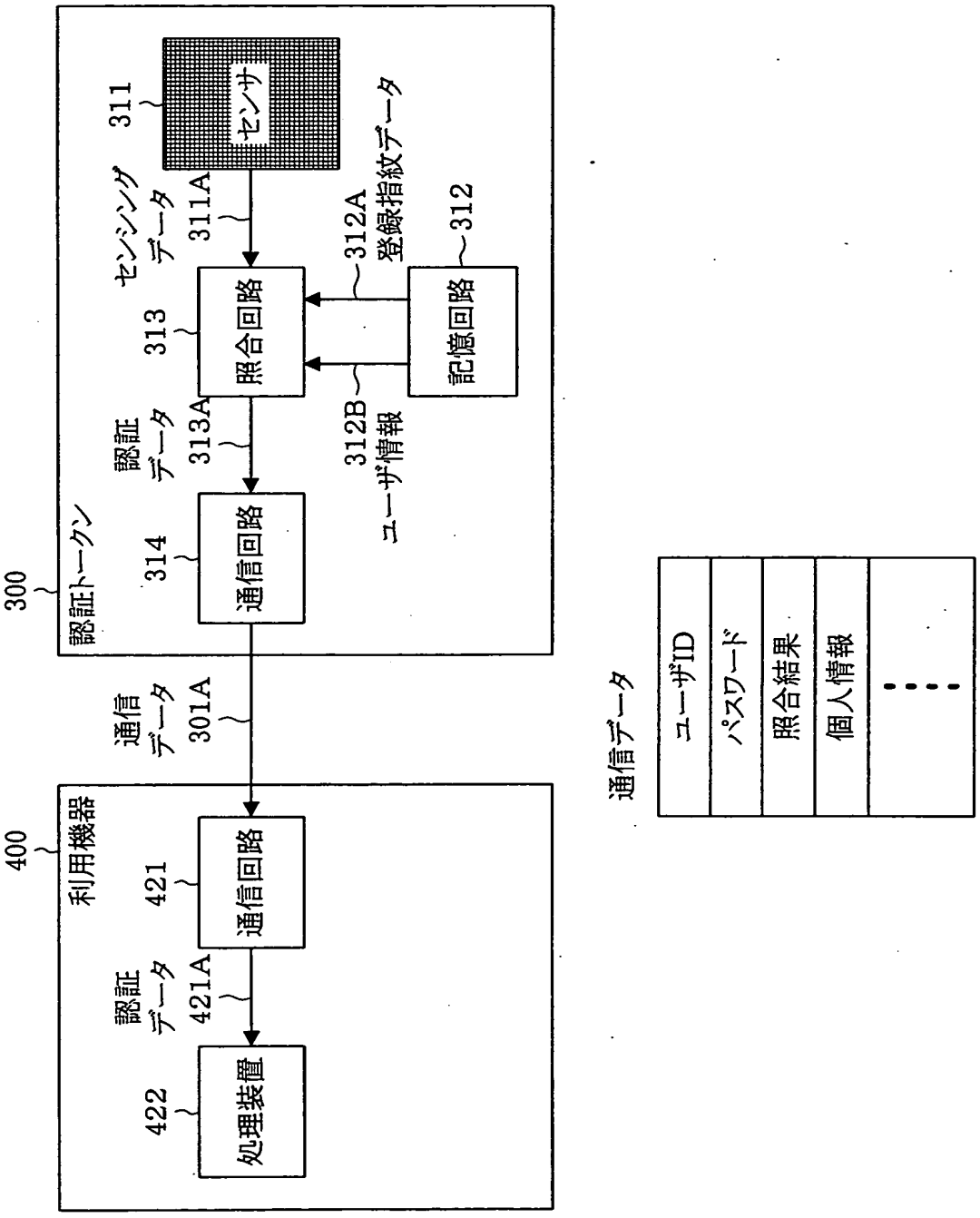
【図１２】


指紋センサ
２０２
２１７
２１７
２１６
２１５
２１５
２１６
２１７
２１４
２１２
２１３
２１３
２１１
２１８
容量検出回路
容量検出回路
２１８
処理装置
２０３

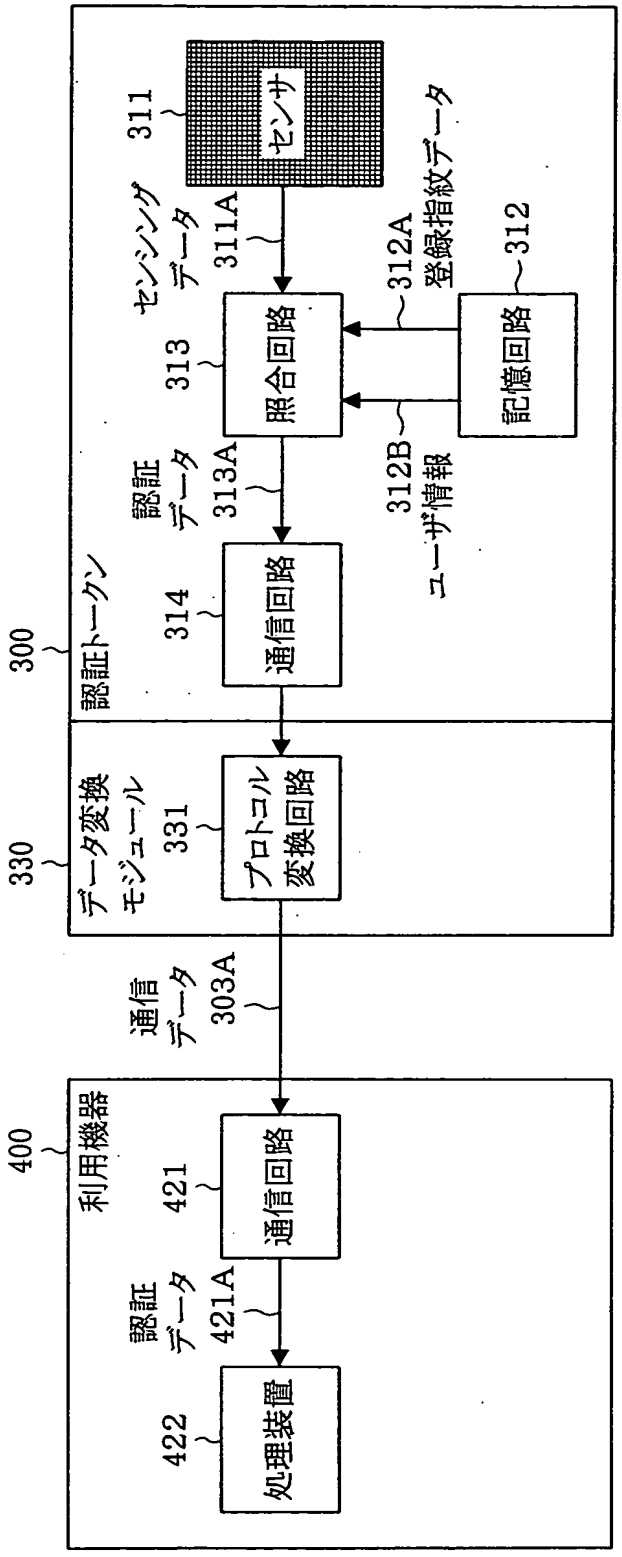
【図１３】


(a)
10
Cf
3
17
215
N1a
VDD
PRE
30
VG
Q1a
N2a
Q2a
VDD
Q4a
41
OUT
Q3a
RE
I
21a
Cp1a
Cp2a
Ra
20
40
(b) PRE
電位
VDD
0
時間
(c) RE
電位
VDD
0
時間
(d) N1a, N2a
電位
N2a
VDD
VG−Vth
N1a
ΔV
0
Δt
時間

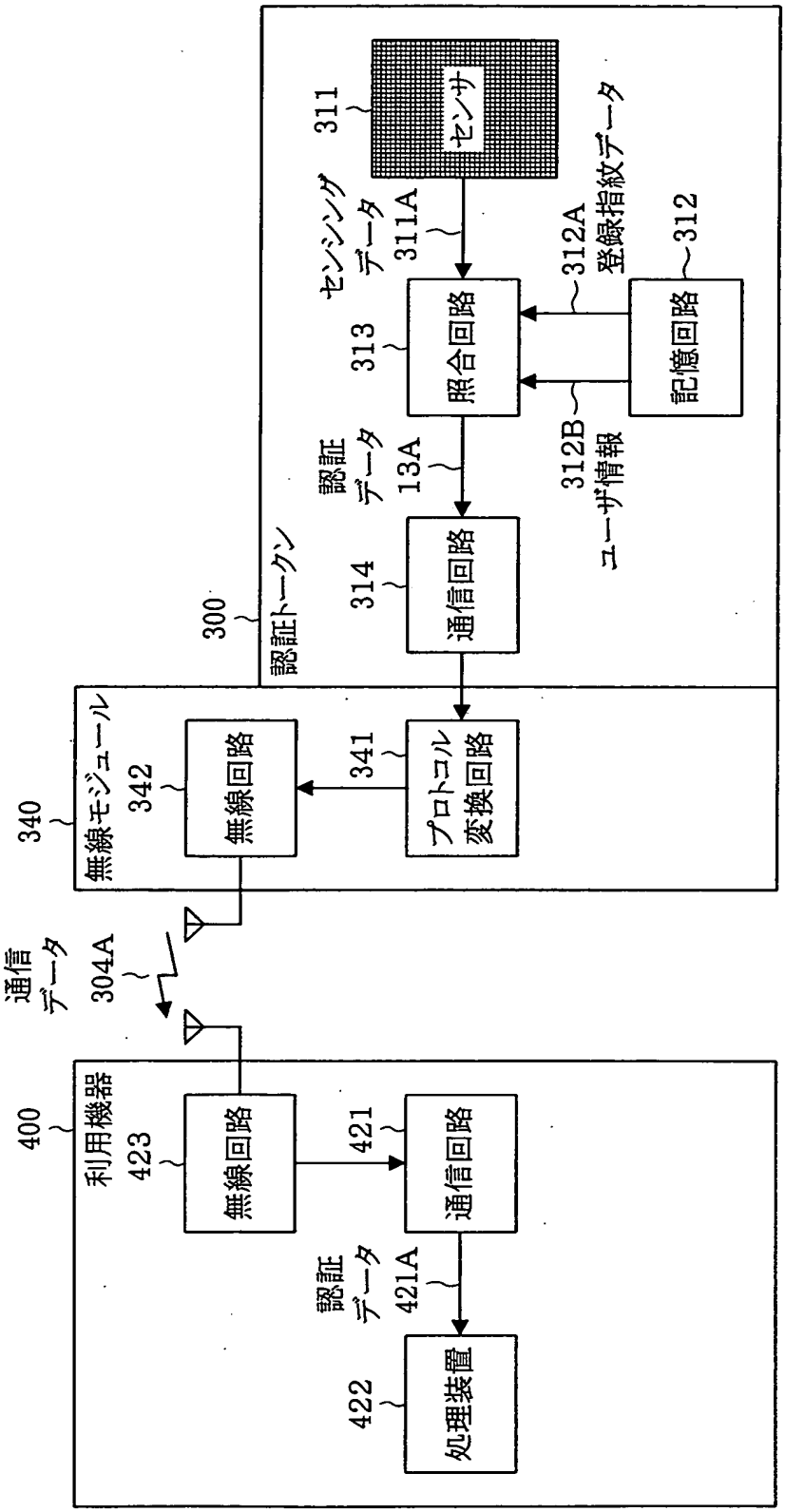
【図１４】


300
認証トークン
311
センサ
センシングデータ
311A
312A
登録指紋データ
312
313
照合回路
記憶回路
認証データ
313A
312B
ユーザ情報
314
通信回路
通信データ
301A
400
利用機器
421
通信回路
認証データ
421A
422
処理装置
通信データ
ユーザID
パスワード
照合結果
個人情報

【図１５】


認証トークン
300
センサ
311
センシングデータ
311A
照合回路
313
記憶回路
312
登録指紋データ
312A
ユーザ情報
312B
認証データ
313A
通信回路
314
データ変換モジュール
330
プロトコル変換回路
331
通信データ
303A
利用機器
400
通信回路
421
認証データ
421A
処理装置
422

【図１６】


認証トークン
300
センサ
311
センシングデータ
311A
312A
登録指紋データ
312
照合回路
313
記憶回路
認証データ
313A
312B
ユーザ情報
通信回路
314
無線モジュール
340
無線回路
342
プロトコル変換回路
341
通信データ
304A
利用機器
400
無線回路
423
通信回路
421
認証データ
421A
処理装置
422

【書類名】　　要約書

【要約】

【課題】　利用者のコンサート会場等への入場の際にチケットのチェックを行う係員を必要とすることなくかつ利用者の速やかな入場を可能にするとともに、第三者による不正な入場を阻止する。

【解決手段】　コンサートのチケット購入時に利用者がその代金を支払うと、データベース102及び指紋認証トークン106にパスワードを記憶し、コンサート会場の入場時に指紋認証トークンにより利用者本人の確認を行い、利用者本人であることが認証されて指紋認証トークンから入場ゲート104近傍の無線／赤外線信号受信装置109へ無線または赤外線信号によるパスワードが送信されると、このパスワードを受信したゲートコントローラ103は、データベースのパスワードとの比較を行い双方のパスワードが一致すると入場ゲート104を開放する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社